Beating gummy fingers

How hard is it to 'spoof' biometric security systems? By **Wendy Atkins**.

Science fiction met reality earlier this year when several suppliers of biometrics products were targeted by researchers intent on gaining false entry to systems protected by their devices. Predictably, a widespread media frenzy followed – but it was not always accurate.

Many observers have criticised the biometrics industry for not taking attempts to 'spoof' its technology seriously. Whilst a small percentage of companies may be guilty of overstating the effectiveness of their technology, a number of industry organisations appear committed to countering fraudulent attacks. As Jim Wayman, director of the Biometric Test Center at San Jose State University, comments: "This has been an area of interest for more than 20 years and we are working on it."

Efforts to overcome spoofing – or biometric forgery – are cited in patent applications, newspaper articles and academic papers dating back to 1981. Recently, the US National Institute of Standards and Technology Facial Recognition Vendor Test 2000 documented the use of photographs to fool face recognition systems.

One way of proving a face presented to a system is alive is by asking the user to smile or blink. But there is a flaw in this thinking, according to Wayman. "Just because the user is alive does not mean the biometric is not a forgery. Consequently, the current US and UK government work on 'Common Criteria' for biometric device evaluation distinguishes between 'mimic' and 'artefact' attacks."

Potential ways of spoofing biometrics include casual attacks, mimicry of biometrics and impostor attacks from dummy 'artefact' biometric features.

- *Casual attacks.* Here, there is no prior preparation and most vendor calculations of false acceptance rates are based on such attacks being successful.
- *Mimicry.* This usually takes place with technologies that require behavioural characteristics to be examined (for instance, dynamic signature and speaker verification). In these instances, the impostor may observe the biometric and, with practice, may succeed in impersonating it.
- *Dummy artefacts.* Potential impostors claim it is relatively easy and inexpensive to duplicate a fingerprint with and without the cooperation of its owner. In the case of cooperative duplication, an individual provides his or her fingerprint voluntarily as a basis for a silicone dummy. Here, there is a strong chance of creating a perfect duplicate, as the original fingerprint is available for comparison with the dummy. Without cooperation, the fingerprint must first be obtained covertly from an object that its owner has touched – potentially a biometric fingerprint scanner. This is much tougher as it is not always possible to get a good image of the print. And even if a good image is obtained, will it be the finger registered to a biometric system?

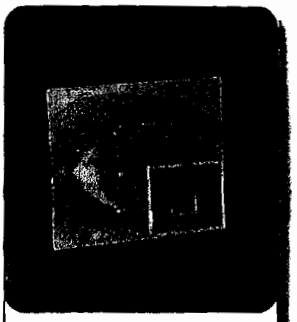
Other forms of attack include attempts to use pictures of registered individuals in front of face recognition devices. These attempts are usually unsuccessful if a face recognition device has a 'liveness' system. However, Ton van der Putte, senior consultant at Dutch company Atos Origin, claims it is possible to fool some systems by stretching a photograph electronically and then bending it for the camera.

Earlier this year, German computing and technology magazine c't published an article by Lisa Thalheim, Jan Krissler and Peter-Michael Ziegler, who claimed they used dummy biometric features successfully on a range of devices. Capacitive fingerprint sensors from five companies were hacked successfully using methods such as breathing on the sensor, pressing a thin walled water filled plastic bag on the sensor surface or dusting the surface of the sensor with graphite powder and pressing down on the resulting print with an adhesive film.

Two optical fingerprint sensors were also targeted. These were fooled by the adhesive film method combined with a halogen lamp. They also suffered from 'gummy finger' attacks using candle wax to take the impression and silicone to make the fake finger.

Additionally, the group tested a thermal fingerprint reader, which they spoofed – with difficulty – using a 'gummy finger'.

Even with a 'liveness' detection system in place, face recognition technology from a German company failed to detect an impostor. Using a video of a registered user moving his head slightly, the researchers managed to fool the system. An iris recognition device fared little better. The device, designed for computer access control, was successfully spoofed by presenting a quality image of an iris (sprayed on to matt inkjet paper), with a hole cut out where the pupil was located. The authors then put the picture up to their own eyes and positioned their pupil into the hole.



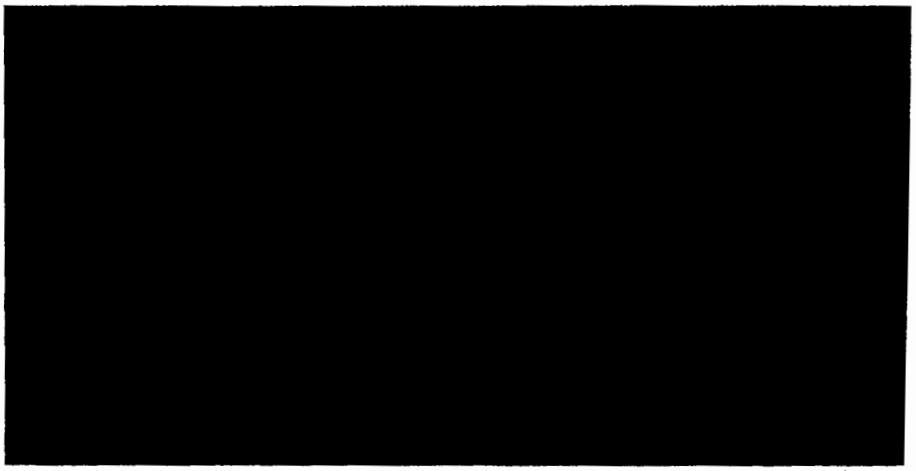
Iris recognition devices have been spoofed using high quality ink jet prints with a hole cut out for the pupil.

Do they or don't they?

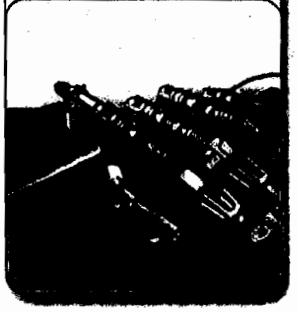
When the mainstream media heard of these stories, it soon published articles with a general tone of 'biometrics don't work'. But, as Richard Norton, executive director of the International Biometrics Industry Association (IBIA), comments: "A lot of people are concerned about the realities and fiction. To a certain extent, some statements made in the media have been inaccurate. But we take it seriously. The question is: do people understand what spoofing is and isn't?"

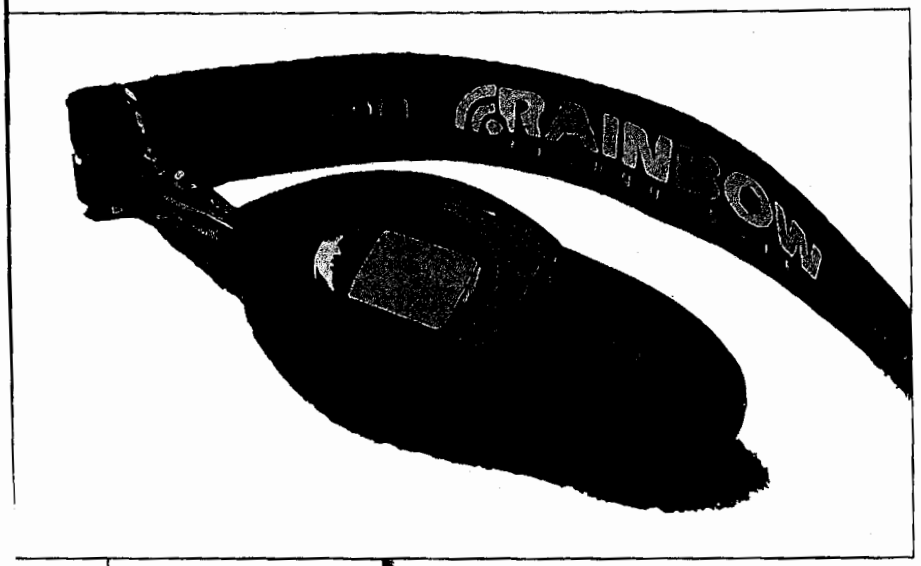
There is no doubt that all forms of security have a degree of vulnerability: A lock on a door could be picked or kicked out of place; a 'secret' PIN could be guessed or found; a magnetic striped bank card could be 'skimmed'. In short, whichever part of security you are involved in, your job is to stay at least one step ahead of potential fraudsters.

And biometrics is no exception. The technology, in common with other forms of security, must provide protection that is sufficiently difficult and costly to overcome that no fraudster would be interested in beating it. Wayman agrees: "If the cost, complexity and execution time of the attack exceed that available to the attacker, their arguments are theoretical only. Why mount a $30,000 attack against the finger geometry system at Disney World when admission is only $50?"



Observers at entry and exit points would have a far greater chance of noticing whether somebody was trying to present an artificial hand.





In order to access systems protected by SuperToken – a concept usb token from Rainbow Technologies – not only do you need the token itself, but you also need to know a password and to have the correct fingerprint.

Can a face recognition system be fooled by stretching a photograph electronically and then bending it for the camera?

Even if the 'return on investment' is considered worthwhile, it is worth remembering that the owner of a dummy finger or face will often have to get through other areas of security before accessing areas such as time and attendance systems, executive facilities or a company's pc network (areas where many biometric devices are currently located).

In the case of pc access control, you would have to get past company security processes as well as colleagues of the person whose fingerprint you had stolen. In fact, it could often be easier to hack into a system. As Yona Flink, founder and ceo of Israeli company OptiSec, says: "In low level security areas, it just wouldn't be worth the hassle. In higher security areas – such as access to tender documents, contract and salaries – you'd need different security levels. For example, you may use layered security such as the left finger, right finger and thumb or you may use a biometric and a smart card."

Another answer may be to have procedures that limit any damage that could occur if an individual's identity is spoofed. According to Jackie Groves, managing director of Hertfordshire based Utimaco Safeware: "This could be achieved by ensuring that, once into a network, a genuine user only has access to relevant applications and, when in those applications, only has access to relevant data."

In high security areas – such as secure access to nuclear reactors, prisons, immigration controls and military facilities – it could be argued that the 'return on investment' would pay off if an individual managed to access or enter these areas illegally. In such cases, it is equally important that operators of these facilities 'beef up' their security accordingly. One answer may be to secure exit points – it is often much tougher to enter a property than it is to leave. It may also be reasonable to place a human observer at entry and exit points. Such a person would have a far greater chance of noticing whether somebody was trying to present a gummy finger or an artificial hand.

How the biometric template is stored should also be considered. "Care should be taken with selection of the complete biometric system, as many require enrolment and matching to be performed by a host system," says Graham Peat, European marketing manager at Rainbow Technologies. "For example, stand alone scanners and keyboards – often recording the biometric template within a database – could be susceptible to attack. Recent technology advances have enabled 'match on board' technologies, where enrolment, matching and storage of templates can all be performed on the device, rather than relying on the host system for these functions."

Additional security could also be found by combining biometrics with other methods – such as smart cards or PINs – to provide two factor authentication. Utimaco's Groves also recommends that spoofing can be minimised by: setting the software sensitivity at an appropriate level to minimise false acceptance rates; ensuring strong authentication at the card issuance time; educating users to understand the rapid response needed when a smart card goes missing; and by choosing the latest chip and sensor technology.

In light of the media revelations about biometrics, some organisations have reviewed whether or not the technology will meet their needs. Some have, rightly, concluded that, for the short term at least, biometrics will not be suitable. Biometrics is not a 'one size fits all' technology, so it is important that companies supplying biometrics solutions find out about their customer's problems by asking questions and observing security (or the lack of it).

Ask yourself this

If you are considering implementing a biometrics based security solution, you should be asking such questions as: what do we hope to achieve?; where do we need to place the devices to achieve those aims?; what is our operating system?; who is using the system?; what experience do they have?; who is going to be using the software?; what knowledge do they have?; and how confident are they?

There will be further attempts to crack biometric systems and, as an authentication technology designed for security and convenience, we should expect nothing less. In the long term, the success of the industry will be determined, in part, by whether it can stay ahead of the hackers and whether good project management skills and technological expertise are used to ensure that systems are deployed effectively. NG